



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Am

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/717,734	11/20/2003	Matthew J. Dye	W1115/20001	8706

3000 7590 05/09/2005
CAESAR, RIVISE, BERNSTEIN,
COHEN & POKOTILOW, LTD.
11TH FLOOR, SEVEN PENN CENTER
1635 MARKET STREET
PHILADELPHIA, PA 19103-2212

EXAMINER

UNGAR, DANIEL M

ART UNIT PAPER NUMBER

2132

DATE MAILED: 05/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/717,734

Applicant(s)

DYE ET AL.

Examiner

Daniel M. Ungar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1:704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 November 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-85 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-85 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 November 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>3/25/04</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED OFFICE ACTION

1. Claims 1-85 have been examined.

INFORMATION DISCLOSURE STATEMENT

2. The information disclosure statement filed 25 March 2004 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

CLAIM OBJECTIONS

3. Claim 40 recites the limitation "SHAH-1" as a hash function. The "Secure Hash Algorithm" also known as the "Secure Hash Standard" goes by the acronyms SHA1 or SHS, but not SHAH1. (see Schneier, page 442).
4. Claim 60 is objected to under 37 CFR 1.75 as being a substantial duplicate of a portion of claim 39. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

CLAIM REJECTIONS - 35 U.S.C. 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.
6. Claims 10, 40, 45, 46, and 52 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention. Claims not treated in the following rejections are rejected due to their dependency on other, rejected claims.

7. Claim 10 recites the limitation, "the output." There is insufficient antecedent basis for this limitation.

8. Claim 40 recites, "a web security system of Claim 39." There is insufficient antecedent basis for a web security system in claim 39.

9. Claim 45 recites the limitation, "a second file representation." It is unclear how there can be a second file representation when there is no first file representation in any antecedent claim.

10. In claim 45 it is unclear how step (e) differs from step (g).

CLAIM REJECTIONS - 35 U.S.C. 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. Claims 1-11 and 13-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Alcorn et al., U.S. Patent Number 5,643,086.

13. Regarding claim 1, Alcorn et al. disclose a method for monitoring a file in a file security system comprising:

providing a first file representation of a file at a first location (see column 2, lines 23-41);
first processing the first file representation to provide signals in accordance with the first file representation, and storing the first signals in a central repository at a second

location remote from the first location (see abstract; column 2, lines 27-32 and 47-52; column 3, lines 22-33; column 6, lines 47-57);
providing a second file representation of the file at a third location remote from the second location (see column 2, lines 57-65; column 3, lines 28-33);
second processing the second file representation to provide second signals in accordance with the second file representation, and accessing the first signals from the central repository and comparing the first and second signals (see column 2, lines 57-65; column 8, lines 1-26); and
determining a status the file in accordance with the comparing (see column 2, lines 62-65).

14. Regarding claim 2, Alcorn et al. disclose the first location being substantially the same as the third location (see column 3, lines 22-33; column 8, lines 1-26).

15. Regarding claims 3, 4, and 5, Alcorn et al. disclose applying a hash function to the first and second file representations, providing corresponding mathematical signatures, and comparing the first and second mathematical signatures (see column 2, lines 43-65; column 7, line 41 – column 8, line 26).

16. Regarding claims 6 and 7, Alcorn et al. disclose comparing substantially the entireties of the first and second file representations and excluding a selected portion of the first and second file representations from the comparing (see column 3, line 58 – column 4, line 19; column 10, lines 30-50).

17. Regarding claims 8-10, Alcorn et al. disclose the file as a data set (abstract; column 2, line 44) and all programs and fixed data stored in memory (see column 3, line 61), meeting the limitation of a database and a combination of files, and output of a program (see column 6, lines 30-40).

18. Regarding claim 11, Alcorn et al. disclose the authentication being repeated periodically (see column 3, lines 13-21; column 4, lines 49-58; column 9, lines 34-50).
19. Regarding claim 13, Alcorn et al. disclose the authentication being repeated in response to a predetermined system event (see column 9, lines 44-47).
20. Regarding claim 14, Alcorn et al. disclose the authentication being repeated in response to manual initiation (see column 3, lines 16-21).
21. Regarding claim 15, Alcorn et al. disclose providing an alert in response to the determining of the status of the file (see column 8, lines 18-26).
22. Claims 19-23, 28-29, 61-63, 67-68, 76, and 84 are rejected under 35 U.S.C. 102(b) as being anticipated by Kojima et al., U.S. Patent Number 5,933,851.
23. Regarding claim 19, Kojima et al. disclose a method for monitoring a file in a file security system, comprising:
 - providing a plurality of files disposed at a plurality of differing locations, each file having a respective location indicator for indicating the location and a respective first file representation (see abstract; column 1, lines 54-62; column 6, lines 26-38; claim 11);
 - first processing each first file representation to provide a corresponding plurality of first signals in accordance with the first file representations (see claim 3);
 - storing the plurality of first signals and respective location indicators in a central repository disposed in a location remote from the differing locations (see column 6, lines 26-38; column 9, lines 42-53);
 - providing a second file representation of a selected file of the plurality of files having a selected location indicator, and second processing the second file representation to provide second signals in accordance with the second file representation (see column 9, lines 6-13; claim 13);

accessing selected first signals of the plurality of first signals from the central repository in accordance with the selected location indicator, and comparing the selected first signals with the second signals (see column 9, lines 42-60);

24. Regarding claim 20, Kojima et al disclose determining a status of the selected file in accordance with the comparing (see column 9, lines 42-60).

25. Regarding claims 21, 22, and 23, Kojima et al. disclose applying a hash function to the first and second file representations, providing corresponding mathematical signatures, and comparing the first and second mathematical signatures (see column 9, lines 13-60).

26. Regarding claim 28, Kojima et al. disclose the file comprising the output of a program (see column 3, lines 35-60).

27. Regarding claim 29, Kojima et disclosed the authentication being repeated periodically (see column 7, lines 44-48; column 8, lines 53-56; column 9, lines 54-60).

28. Regarding claim 31, Kojima et al. disclose providing a second file representation in response to a predetermined system event (see column 6, lines 26-38).

29. Regarding claim 33, Kojima et al. disclose providing an alert in response to determination of status (see column 8, lines 12-31).

30. Regarding claim 61, Kojima et al. disclose a method for monitoring a file in a file security system, comprising:

providing a first file representation of a file at a first location (see abstract; column 1, lines 54-62; column 6, lines 26-38; claim 11);

first processing the first file representation to provide first signals in accordance with the first file representation (see claim 3);

storing the first signals in a central repository disposed at a second location which is remote from the first location (see column 6, lines 26-38; column 9, lines 42-53);
notifying the second location of a change in the file (see column 7, lines 49-58);
altering the first signals in accordance with the notifying to provide altered first signals (see column 7, line 66 – column 8, line 5);
accessing the altered first signals from the central repository and determining a status of the file in accordance with the altered first signals (see column 8, lines 12-31).

31. Regarding claim 62, Kojima et al. disclose providing a second file representation of the file, and second processing the second file representation to provide second signals in accordance with the second file representation (see column 9, lines 6-13; claim 13); and comparing the altered first signals with the second signals and determining the status of the file in accordance with the comparing (see claim 13).

32. Regarding claim 63, Kojima et al. disclose applying a hash function to the first and second file representations, providing corresponding mathematical signatures, and comparing the first and second mathematical signatures (see column 9, lines 13-60).

33. Regarding claim 67, Kojima et al. disclose the file comprising the output of a program (see column 3, lines 35-60).

34. Regarding claim 68, Kojima et al. disclosed the authentication being repeated periodically (see column 7, lines 44-48; column 8, lines 53-56; column 9, lines 54-60).

35. Regarding claim 70, Kojima et al. disclose providing a second file representation in response to a predetermined system event (see column 6, lines 26-38).

36. Regarding claim 72, Kojima et al. disclose providing an alert in response to determination of status (see column 8, lines 12-31).

37. Regarding claim 76, Kojima et al. disclose notifying using HTTP (see column 6, lines 51-55).

38. Regarding claims 81-83, Kojima et al. disclose notification prior to, simultaneous with, and after a change (see column 6, lines 56-67; column 7, lines 49-58; column 8, lines 6-35);

39. Regarding claim 84, Kojima et al. disclose the change occurs on a scheduled basis (see column 6, lines 11-17 and lines 26-38).

40. Claims 39, 42, 43, 45, 46, 59, and 60 are rejected under 35 U.S.C. 102(b) as being anticipated by Smithies et al., U.S. Patent Number 5,647,017.

41. Regarding claim 39, Smithies et al. disclose a method for monitoring a file in a file security system comprising:
providing a file to be monitored (see abstract; claim 1);
applying a plurality of hash functions to the file to provide a plurality of file signatures (see abstract; column 4, lines 33-46);
applying a time varying stamp to at least one of the file signatures to provide a time stamped signature, combining the file signatures of the plurality of signatures including the time stamped file signature to provide a combined file signature, and applying a hash function to the combined file signature to provide a hashed file signature (see abstract; column 9, lines 40-47; column 10, lines 29-54; column 13, lines 42-53); and
comparing the hashed file signature with a further file signature (see claims 2, 3, and 8);

42. Regarding claims 42 and 43, Smithies et al. disclose changing the time varying stamp daily and storing a plurality of time varying stamps for use in subsequent comparisons of the file signature with differing signatures (see abstract; column 4, line 63 - column 5, line 3; column 10, line 31; column 13, lines 61-63; claim 22).

43. Regarding claim 45, Smithies et al. disclose:
providing a second file representation to be monitored (see claims 2 and 3);
applying the plurality of hash functions to the second file representation to provide a plurality of further file signatures (see abstract; column 4, lines 33-46; claims 2 and 3);
applying a hash function to the further combined file signature to provide a further hashed file signature (see abstract; column 13, lines 42-53; claims 2 and 3); and
comparing the hashed file signature with a further file signature, determining a status of the file in accordance with the comparing (see claims 2, 3, and 8);

44. Regarding claim 46, Smithies et al. disclose storing the hashed signature in a central repository disposed at a location remote from the file (see column 5, lines 4-12; column 7, lines 53-65).

45. Regarding claim 59, Smithies et al. disclose applying a pass phrase to at least one of the file signatures (see column 18, lines 20-27).

46. Regarding claim 60, Smithies et al. disclose applying a time indicating stamp to at least one of the file signatures (see abstract; column 9, lines 40-47; column 10, lines 29-54).

CLAIM REJECTIONS - 35 U.S.C. 103(a)

47. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alcorn et al., as established above, in view of Takeda et al., U.S. Patent Number 6,071,191.

48. Regarding claim 12, Alcorn et al. do not disclose authentication repeated continuously. However, in a similar field of endeavor, Takeda et al. disclose a system of monitoring and authenticating in a network setting on a continuous basis (abstract; column 1, lines 48-60). In light of the teachings of Takeda et al. it would have been an obvious modification to the method of Alcorn et al. to provide the authentication continuously to enhance security by not allowing a time lapse in authentication.

49. Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alcorn et al., as established above, in view of Scott, U.S. Patent Application Publication Number 2001/0044820.

50. Regarding claim 16, Alcorn et al. fail to disclose restoring the file in response to the determining status of the file. However, Scott discloses a method of monitoring web sites, in which after determining a file is altered by comparing a hash, the file can be restored (see claim 19). In light of the teaching of Scott it would have been obvious to one of ordinary skill in the art at the time of the invention to allow restoring in the method of Alcorn et al. if the status is determined to be an alteration in the file in order to not allow the corrupted or unauthentic file to stay in the system, an object of Alcorn (see Alcorn, column 8, lines 20-26).

51. Regarding claims 17 and 18, Alcorn et al. do not disclose a web site with web addresses and traversal using a spider. Nevertheless, Scott discloses the file or plurality of files to be authenticated disposed in a web site with web site addresses which correspond to physical addresses (see abstract; paragraphs 0023, 0035, 0036). Scott discloses traversing the web site using a spider (see paragraph 0036). In light of the teaching of Scott it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Alcorn et al. to monitor files particularly in web sites in addition to other files in order to provide the same authentication to ensure the integrity of the files.

52. Claims 24-25, 31-33, 64, and 70-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kojima et al., as established above, in view of Alcorn et al., U.S. Patent Number 5,643,086.

53. Regarding claims 24 and 25, Kojima et al. do not disclose comparing substantially the entireties of the first and second file representations or excluding a selected portion of the first and second file representations from comparing. Nevertheless, in a similar field of endeavor,

Alcorn et al. disclose comparing substantially the entireties of the first and second file representations and excluding a selected portion of the first and second file representations from the comparing (see column 3, line 58 – column 4, line 19; column 10, lines 30-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Kojima et al. to compare substantially the entireties of the first and second file representations to compare more thoroughly or to exclude portions of the files in order to save time and unnecessary processing power.

54. Regarding claim 32, Kojima et al. do not disclose providing a second file representation by manual initiation. Nevertheless, Alcorn et al. disclose the authentication being in response to manual initiation (see column 3, lines 16-21). In light of the teaching of Alcorn et al. it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Kojima et al. to be able to initiate authentication manually to provide authentication whenever it is needed.

55. Regarding claim 64, Kojima et al. do not disclose excluding a selected portion of the first and second file representations from comparing. Nevertheless, in a similar field of endeavor, Alcorn et al. disclose excluding a selected portion of the first and second file representations from the comparing (see column 10, lines 30-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Kojima et al. to exclude portions of the files in order to save time and unnecessary processing power.

56. Regarding claim 71, Kojima et al. do not disclose providing a second file representation by manual initiation. Nevertheless, Alcorn et al. disclose the authentication being in response to manual initiation (see column 3, lines 16-21). In light of the teaching of Alcorn et al. it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Kojima et al. to be able to initiate authentication manually to provide authentication whenever it is needed.

57. Claims 26, 27, 34-38, 65, 66, 73-75, 78-79, and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kojima et al., as established above, in view of Scott, U.S. Patent Application Publication Number 2001/0044820.

58. Regarding claims 26 and 27, Kojima et al. fail to disclose the file comprising a database or a combination of files. Nevertheless, Scott discloses the file comprising a database or combination of files (see paragraph 0035). It would have been obvious to one of ordinary skill in the art at the time of the invention to have specified the method of Kojima et al. to provide for authenticating files comprising databases or combinations of files in order to monitor the entire web page which consists of databases and multiple files, as disclosed by Scott (see paragraph 0035).

59. Regarding claim 34, Kojima et al. fail to disclose restoring the file in response to the determining status of the file. However, Scott discloses a method of monitoring web sites, in which after determining a file is altered by comparing a hash, the file can be restored (see claim 19). In light of the teaching of Scott it would have been obvious to one of ordinary skill in the art at the time of the invention to allow restoring in the method of Kojima et al. if the status is determined to be an alteration in the file in order to not allow the corrupted or unauthentic file to stay in the system.

60. Regarding claims 35-38, Kojima et al. do not disclose a web site with web addresses and location indicators and traversal using a spider. Nevertheless, Scott discloses the file or plurality of files to be authenticated disposed in a web site with web site addresses which correspond to physical addresses and location indicators to access the first signals (see abstract; paragraphs 0023, 0035, 0036). Scott discloses traversing the web site using a spider (see paragraph 0036). In light of the teaching of Scott it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Kojima et al. to monitor files particularly in web sites in addition to other files in order to provide the same authentication to ensure the integrity of the files.

61. Regarding claims 65 and 66, Kojima et al. fail to disclose the file comprising a database or a combination of files. Nevertheless, Scott discloses the file comprising a database or combination of files (see paragraph 0035). It would have been obvious to one of ordinary skill in the art at the time of the invention to have specified the method of Kojima et al. to provide for authenticating files comprising databases or combinations of files in order to monitor the entire web page which consists of databases and multiple files, as disclosed by Scott (see paragraph 0035).

62. Regarding claim 73, Kojima et al. fail to disclose restoring the file in response to the determining status of the file. However, Scott discloses a method of monitoring web sites, in which after determining a file is altered by comparing a hash, the file can be restored (see claim 19). In light of the teaching of Scott it would have been obvious to one of ordinary skill in the art at the time of the invention to allow restoring in the method of Kojima et al. if the status is determined to be an alteration in the file in order to not allow the corrupted or unauthentic file to stay in the system.

63. Regarding claims 74 and 75, Kojima et al. do not disclose a web site with web addresses and location indicators and traversal using a spider. Nevertheless, Scott discloses the file or plurality of files to be authenticated disposed in a web site with web site addresses which correspond to physical addresses and location indicators to access the first signals (see abstract; paragraphs 0023, 0035, 0036). Scott discloses traversing the web site using a spider (see paragraph 0036). In light of the teaching of Scott it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Kojima et al. to monitor files particularly in web sites in addition to other files in order to provide the same authentication to ensure the integrity of the files.

64. Regarding claim 78, Kojima et al. do not disclose notification via HTTPS, but Scott discloses notification via SSL (HTTPS). It would have been obvious to one of ordinary skill in the art at the time of the invention to have used HTTPS instead of regular HTTPS for a more secure protocol.

65. Regarding claim 79, Kojima et al. do not disclose notification via SMTP, but Scott discloses notification via STMP. It would have been obvious to one of ordinary skill in the art at the time of the invention to have used STMP, an efficient notification protocol.

66. Regarding claim 85, Kojima et al. do not specify the notification over pre-agreed protocols and transports, but Scott discloses using pre-agreed protocols over pre-agreed transports to notify (see paragraphs 0046 and 0047). It would have been obvious to one of ordinary skill in the art at the time of the invention to have used pre-agreed protocols over pre-agreed transports to notify in order that the notification take place smoothly.

67. Claims 30 and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kojima et al., as established above, in view of Takeda et al., U.S. Patent Number 6,071,191. Kojima et al. do not disclose authentication repeated continuously. However, in a similar field of endeavor, Takeda et al. disclose a system of monitoring and authenticating in a network setting on a continuous basis (abstract; column 1, lines 48-60). In light of the teachings of Takeda et al. it would have been an obvious modification to the method of Kojima et al. to provide the authentication continuously to enhance security by not allowing a time lapse in authentication.

68. Claims 77 and 80 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kojima et al., as established above, in view of Pugliese III et al., U.S. Patent Application Publication Number 2001/0044751. Kojima et al. fail to disclose notification via XML transactions or a transaction website. However, notification via XML transactions or transaction websites were well known in the art at the time of the invention. Exemplary of this is Pugliese III et al. who disclose notifications via XML transactions and transaction websites (see paragraph 0259, 0293). It would have been obvious to one of ordinary skill in the art at the time of the invention to have used XML and transaction websites, which are efficient and standard methods of notification.

69. Claims 40, 47-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smithies et al., as established above, in view of Alcorn et al., U.S. Patent Number 5,643,086.

70. Regarding claim 40, Smithies et al. disclose using the MD5 algorithm (see column 20, lines 28-31), but not the SHA1 or MD2 algorithms. However, it was well known in the art at the time of the invention that SHA1 and MD2 are equivalent to MD5. Exemplary of this is Alcorn et al. who disclose the use SHA, MD2, and MD5 algorithms (see column 7, lines 45-49). It would have been obvious to one of ordinary skill in the art at the time of the invention to have substituted the MD5 algorithm for MD2 or SHA1, equivalent hash algorithms.

71. Regarding claims 47 and 48, Smithies et al. do not disclose the hashed signature and further signature representative of substantially the entireties of the file or a selected portion of the file. Nevertheless, in a similar field of endeavor, Alcorn et al. disclose comparing substantially the entireties of the first and second files and excluding a selected portion of the first and second files (see column 3, line 58 – column 4, line 19; column 10, lines 30-50). It would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Smithies et al. to compare substantially the entireties of the file signatures to compare more thoroughly or to exclude portions of the file in order to save time and unnecessary processing power.

72. Regarding claims 49-51, Smithies et al. do not disclose the file to be a database, combination of files, or output of a program. However, Alcorn et al. disclose the file as a data set (abstract; column 2, line 44) and all programs and fixed data stored in memory (see column 3, line 61), meeting the limitation of a database and a combination of files, and output of a program (see column 6, lines 30-40). In light of the teaching of Alcorn et al. it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Smithies et al. to monitor databases, combinations of files, and program outputs in order to utilize the authentication method with regard to a wide range of files.

73. Regarding claims 52 and 53, Smithies et al. fail to disclose determining the second file representation periodically. However, Alcorn et al. disclose the authentication being repeated periodically (see column 3, lines 13-21; column 4, lines 49-58; column 9, lines 34-50), and Alcorn et al. disclose providing an alert in response to the determining of the status of the file (see column 8, lines 18-26). In light of the teaching of Alcorn et al. it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Smithies et al. to repeat the authentication process at certain times to provide the security the authentication affords when it is needed, and to provide an alert so that if an intrusion is detected it can be attended to.

74. Claims 41 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smithies et al., as established above, in view of Tessman Jr. et al., U.S. Patent Application Publication Number 2002/0135801. Smithies et al. do not disclose interspersing the file signatures with random characters, but using random characters to obtain a predetermined length from a hash function was well known in the art at the time of the invention. Exemplary of this is Tessman Jr. et al. who disclose inserting random characters into a signature to create a hash of a predetermined length. In light of the teaching of Tessman Jr. et al. it would have been obvious to one of ordinary skill in the art at the time of the invention to have used random characters in order to achieve the predetermined length of the hash.

75. Claims 54-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Smithies et al., as established above, in view of Scott, U.S. Patent Application Publication Number 2001/0044820.

76. Regarding claim 54, Smithies et al. fail to disclose restoring the file in response to the determining status of the file. However, Scott discloses a method of monitoring web sites, in which after determining a file is altered by comparing a hash, the file can be restored (see claim

19). In light of the teaching of Scott it would have been obvious to one of ordinary skill in the art at the time of the invention to allow restoring in the method of Smithies et al. if the status is determined to be an alteration in the file in order to not allow the corrupted or unauthentic file to stay in the system.

77. Regarding claims 55 and 56, Smithies et al. do not disclose a web site with web addresses and traversal using a spider. Nevertheless, Scott discloses the file or plurality of files to be authenticated disposed in a web site with web site addresses which correspond to physical addresses (see abstract; paragraphs 0023, 0035, 0036). Scott discloses traversing the web site using a spider (see paragraph 0036). In light of the teaching of Scott it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Smithies et al. to monitor files particularly in web sites in addition to other files in order to provide the same authentication to ensure the integrity of the files.

78. Regarding claims 57 and 58, Smithies et al. do not disclose applying a digital signature to a certificate to at least one file signature. Nevertheless, protecting a file signature with a digital signature and certificate was well known in the art at the time of the invention. Exemplary of this is Fisher, who discloses applying a digital signature to a file signature (see abstract; column 7, lines 13-20 and 51-62), and applying a certificate to the digital signature (see column 2, lines 19-37; column 5, lines 59-68). In light of the teaching of Fisher it would have been obvious to one of ordinary skill in the art at the time of the invention to have modified the method of Smithies et al. to add a digital signature and certificate to make the signature more secure.

CONCLUSION

79. The following art cited and not relied upon is considered relevant to applicants' invention:

Haber et al., U.S. Patent Number 5,136,647

Fischer, U.S. Patent Number 5,422,953

Cooper et al., U.S. Patent Application Publication Number 2001/0051996

80. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel M. Ungar whose telephone number is 571.272.7960. The examiner can normally be reached on 8:30 - 6:00 Monday - Thursday, Alt. Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571.272.3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit 2132

DMU
Daniel M. Ungar

Gilberto Barron Jr.
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100